## *3.3 External Interface Requirements*

### 3.3.1 Alert Services External Interface Requirements

The Alert Services modules shall provide an open, public software interface (API) between the applications programs and all Alert Services capabilities (see Figure 1).

Traceability:
Priority ???

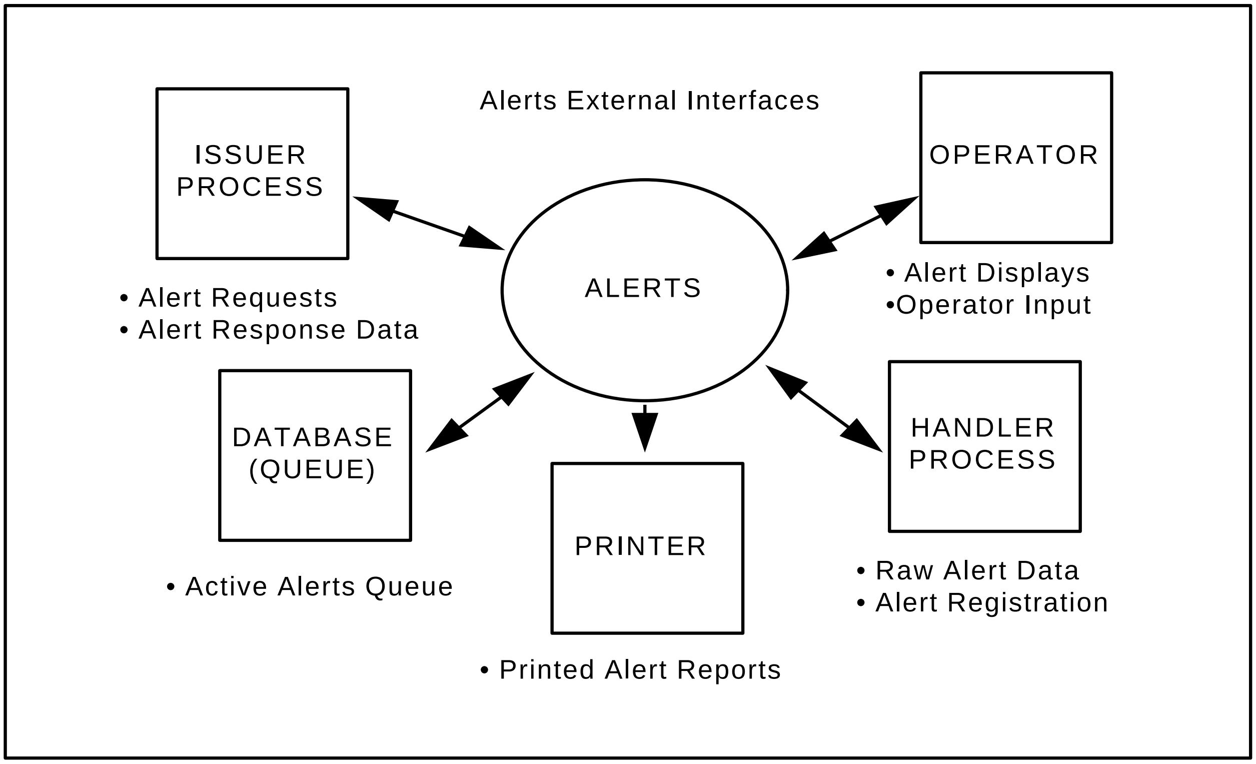

**Figure 1. Alerts Manager External Interfaces**

### 3.3.2 Track Correlation Management Services External Interface Requirements

The following apply to the Track Correlation Managment Services (or System), abbreviated TCMS.

Functionality of the database **shall** include transmission and receipt of messages via Communication Services/Data Exchange Services, and database maintenance via the Data Management Services. This functionality must exist for real-world, simulated, and live-training tracks.

Traceability:
Priority ???

### 3.3.2.1 Interface Identification and Diagrams

### 3.3.2.2 Data Retrieval/Update Interface

3.3.2.2.1 Data sources **shall** include TADIXS, OTCIXS, RADAR, ACDS, JSTARS, PLRS/EPLRS, TRAP/TDDS, TIBS, TRIXS, SIPRNET, JWICS, IBS, and TADIL networks. The TCMS **shall** support processing for national system reporting of tactical ballistic missile (TBM) data.

Traceability:
Priority ???

3.3.2.2.2 The TCMS **shall** provide the ability to choose a communications channel for transmission.

Traceability:
Priority ???

3.3.2.2.3 The architecture **shall** support high data rates and large amounts of data. It **shall** be scaleable. As such, no software changes and minimal system modifications **shall** be required to accommodate additional data sources or increases in data bandwidth.

Traceability:
Priority ???

3.3.2.2.4 The TCMS **shall** support dynamically changing bandwidth availability in the backbone WAN.

Traceability:
Priority ???

3.3.2.2.5 The TCMS **shall** track the sensor source at the report level. Any amplifying reports that are generated **shall** also display the source of the information, e.g., link network.

Traceability:
Priority ???

3.3.2.2.6 The TCMS **shall** accommodate multiple tactical receiver data feeds.

Traceability:
Priority ???

### 3.3.2.3 External Segment Data Interaction

3.3.2.3.1 The TCMS **shall** manage objects and additional information related to tracks, (e.g. overlays, PIMs and SOF/SORTS) and provide links to external applications such as MIDB. These links **shall** provide a path for the external applications to "related objects" with the server and request objects registered by another application. For Forces, the TCMS **shall** maintain relationships between force structures and tracks and tie the tracks to the force distributions.

Traceability:
Priority ???

3.3.2.3.2 The TCMS **shall** support the capability to query remote databases (such as JMIE, Wrangler) for information by vessel name, ID number, ID type, flag, time span, and geographical area. The TCMS **shall** support the ability to select from a list of previously sent queries and to load those parameters.

Traceability:
Priority ???

3.3.2.3.3 The TCMS **shall** support the viewing of track reports received from remote databases. The TCMS **shall** support the comparison of these tracks and merging tracks that have identical track names and DTGs. The TCMS **shall** support the selection and addition of the tracks received from remote databases to the system track database.

Traceability:
Priority ???

3.3.2.3.4 The TCMS **shall** provide correlation engine services to external applications.
Traceability:
Priority ???

3.3.2.3.5 The TCMS **shall** provide a two way linkage between other segments and itself. This linkage will allow data sets to be filtered and distributed to the applications that need them, while maintaining access to the entire data set for every segment.
Traceability:
Priority ???

3.3.2.3.6 The TCMS **shall** support APIs to permit mission applications to perform the following functions:

- Submit a contact report to the correlation service.
  Traceability:
  Priority ???

- Set event masks to request notification of specific correlation events (e.g. track update events or new track creation events).
  Traceability:
  Priority ???

- Provide a user interface to manually modify selected track attributes.
  Traceability:
  Priority ???

- Merge tracks.
  Traceability:
  Priority ???

- Compare the attribute data in two or more tracks.
  Traceability:
  Priority ???

- Delete selected track history points.
  Traceability:
  Priority ???

- Delete tracks from the track data base.
  Traceability:
  Priority ???

- Return the currently archived track history of a selected track.
  Traceability:
  Priority ???

- Return all attribute data associated with a track.
  Traceability:
  Priority ???

- Return all attribute data associated with any report in the track history.
  Traceability:
  Priority ???

### 3.3.3 Joint Mapping Tool Kit (JMTK) External Interface Requirements

GCCS working groups are identifying the external interface requirements among the COE areas. The GCCS/JMTK will:

- be implemented using approved system APIs to support integration with the GCCS COE through the mission applications.

  Traceability:
  Priority ???

- be scaleable and provide a path for future upgrades.

  Traceability:
  Priority ???

- provide users the same level of service (i.e., capabilities and responsiveness), regardless of their physical location in the distributed environment).

  Traceability:
  Priority ???

At this juncture, GCCS/JMTK external interface requirements have been identified as shown below.

#### 3.3.3.1 GCCS Internal Infrastructure (COE, Kernel, & Common Support Applications)

These include file management, printing services, presentation services, data interchange services, and database services.

Traceability:
Priority ???

#### 3.3.3.2 GCCS Embedded Functionality

These include multimedia and Web browsers.

Traceability:
Priority ???

#### 3.3.3.3 GCCS Mission Area Applications

- Application Programming Interface (API)

  Traceability:
  Priority ???

- Global Status of Resources and Training System (GSORTS)

  Traceability:
  Priority ???

- Global Transportation Network (GTN)

  Traceability:
  Priority ???

- Joint Defense Intelligence Support Services (JDISS)

  Traceability:
  Priority ???

- Tactical Analysis Replanning Graphical Execution Toolbox (TARGET)

  Traceability:
  Priority ???

Additional interface identification and diagrams will be included in future releases of this SRS as the specific information becomes available.

### 3.3.3.4 CINC/Service/Agency (C/S/A) Unique Applications

Several Service/Agency unique applications are under negotiation as of this release date. More details will be provided in the next release of this document.

### 3.3.3.5 Site-Unique Applications

Several site unique applications are in progress. More details will be provided in the next release of this document.

### 3.3.3.6 Other DoD System Initiatives

Several other DoD system initiatives are currently being reviewed and coordinated. More details will be provided in the next release of this document.

### 3.3.4 Message Processing External Interface Requirements

### 3.3.4.1 Message Processing Interfaces

The message processing module interfaces with the COE-supplied Communications module to receive messages for further processing and hands off new messages to the communications module for transmission. The message processing module also interfaces with processes, which include COE-supplied system services, DBMS, user interaction, alerts, etc., for passing processed message information to the system for action. The message processor receives data from system processes for use in message generation. Internally, the message processor interfaces to low level modules to accomplish requirements listed above.

### 3.3.4.2 Message Processing Interface Identification

MP 3.3.2.1 The message processing module shall interface with the communications area for receipt of and hand off of messages for transmission to external systems

Traceability:
Priority ???

MP 3.3.2.2 The message processing module shall interface with the security administration software for receipt of access control information

Traceability:
Priority ???

MP 3.3.2.3 The message processing module shall interface with the audit software for storage and manipulation of audit information

Traceability:
Priority ???

MP 3.3.2.4 The message processing module shall alternatively provide an interface to a text processing subsystem to generate freetext messages.

Traceability:
Priority ???

MP 3.3.2.5 The message processing module shall alternatively provide an interface to the Office Automation e-mail subsystem for message distribution and introduction of messages to be released.

Traceability:
Priority ???

MP 3.3.2.6 The message processing module shall interface with COE system and application support modules to receive and transmit messages. Specific modules include:

a. Queuing mechanisms (Distributed Computing Services)

Traceability:
Priority ???

b. Alerts

Traceability:
Priority ???

c. Security Services

Traceability:
Priority ???

d. Database Administration

Traceability:
Priority ???

e. MCG&I

Traceability:
Priority ???

f. Office Automation

Traceability:
Priority ???

g. Communications

Traceability:
Priority ???

MP 3.3.2.7 As appropriate, the message processing module shall receive, generate, validate, and distribute the following communications message formats/standards:

a. ACP-126

Traceability:
Priority ???

b. ACP-126 (modified)

Traceability:
Priority ???

c. ACP-127

Traceability:
Priority ???

d. JANAP 128

Traceability:
Priority ???

e. MTS

Traceability:
Priority ???

f. DOI-103

Traceability:
Priority ???

g. ACP-123

Traceability:
Priority ???

h. DD173

Traceability:
Priority ???

i. ACP-127 (modified)

Traceability:
Priority ???

j. IEWCOMCAT

Traceability:
Priority ???

MP 3.3.2.8 The message processing module shall provide an interface to an on-line message storage device

Traceability:
Priority ???

MP 3.3.2.9 The message processing module shall interface with functional applications in order to deliver message data.

Traceability:
Priority ???

### 3.3.5 Office Automation External Interface Requirements

Many other functional areas within the DII COE use office automation software as part of their overall package. For example, the message processing area incorporates a word processor for message composition and the executive manager incorporates a foldering system for file management. As the office automation functional area permeates the integration of other areas, it is important that each of the other functional areas review and update the requirements contained in the Office Automation portions of this document in order to ensure that the requirements meet their needs.

If DII intends to use common office automation modules throughout the COE, then these other functional areas will need to migrate their current products to the DII office automation suite once the requirements process has resulted in product selection. In addition, any future product upgrade and/or change will require coordination between these functional areas.

Office automation APIs will be published, at the appropriate time, in the DII Developer's Kit. DII COE functional areas which make use of those APIs will document their use in a runtime interface document to facilitate version upgrades or migration from one office automation package to another.

Other areas which have external interfaces include the desktop and the data interchange areas. Data interchange will provide the common interchange formats that the office automation software must incorporate. Data interchange requirements have been set forth in the functional requirements for each of the office automation components.

The office automation software area requires that the desktop area support the Common Desktop Environment (CDE) and the Application Programming Interfaces for Windows (APIW) interfaces. The CDE provides end users with a consistent graphical user interface across their workstations, and software developers with a single set of programming interfaces to desktop integration. CDE also enables users to transparently access data and applications for anywhere on the network. APIW specifies the existing practice for application programming interfaces used by a significant majority of programs: the Microsoft Windows APIs. Work on the specification (currently in draft) is occurring via a Technical Committee which has plans to publish a specification in early 1996.

Traceability:
Priority 1

The Office Automation functional area also requires that the X/Open Single UNIX Specification (SUS) be supported and available to the office automation software within this functional area. The X/Open SUS focuses on application portability and will supersede the currently X/Open Portability Guide 4 (XPG4) .

Traceability:
Priority 1

### 3.3.6 On-Line Support Services External Interface Requirements

OL 3.3.1 The On-Line Support segment shall employ standard Application Program Interfaces (APIs) to provide interoperability between itself and other applications.

Traceability:
Priority 1

## *3.4 Internal Interface Requirements*

### 3.4.1 Alerts Services Requirements

AS 3.4.1.1 Distributed Computing Environment (DCE) Remote Procedure Calls (RPCs) shall be used to connect the Alert Servers with Alert Services Clients and DCE Cell Directory Services shall be used to manage the locations of Alert Services servers and backup servers.

Traceability:
Priority ???

### 3.4.2 Track Correlation Management Services Internal Interface Requirements

3.4.2.1 Within the COE, the Track Correlation Management Service (TCMS) has three primary internal interfaces, with communications, message processing and the tactical plotting components of Mapping, Charting Geodesy and Imagery (MCG&I). Correlation **shall** receive parsed data from the message decoding components of the COE on contact reports and track management directives for processing into the Tdb. Correlation **shall** provide data to message encoding components of the COE for formatting and transmission on contact reports and track management directives aimed at reporting and maintaining the COP.

Traceability:
Priority ???

3.4.2.2 Correlation **shall** make data in the Tdb available to the tactical plotting area of MCG&I for geographic display on top of MCG&I products.

Traceability:
Priority ???

3.4.2.3 The Track Correlation Management Service requires support from communications and message processing services, to include support of the encoding and decoding of high volume binary data streams to include TADIL A, B, J, and other high data rate inputs. This requirement is necessary to achieve the required throughput.

Traceability:
Priority ???

3.4.2.4 The COE should provide support for the aggregation of security label attributes (e.g., hierarchical classification, caveats, codewords, handling instructions).

Traceability:
Priority ???

### 3.4.3 Joint Mapping Tool Kit (JMTK) Internal Interface Requirements

All internal interfaces will be handled through the API calls.

### 3.4.5 Office Automation Internal Interface Requirements

The DII Office Automation software packages shall be able to exchange data using cut-and-paste between the applications as well as be able to interchange data via data interchange formats as specified within each package. The requirements for internal data elements within the individual office automation packages are contained in the requirements for each package.

Traceability:
Priority 1

### 3.4.6 On-Line Support Services Internal Interface Requirements

OL 3.4.1 The On-Line Support segment shall employ standard APIs to provide internal interfaces between all applications.

Traceability:
Priority 1

## *3.5 Internal Data Requirements*

### 3.5.4 Message Processing Internal Data Requirements

All message processing components shall be automatically derived from an electronic data representation of the associated message standard, when it exists.

Traceability:
Priority ???

## *3.6 Adaptation Requirements*

### 3.6.1 Alert Services Adaptation Requirements

Alert Services software shall be coded in ANSI Ada 83 and implemented using Open Systems standards. Alert Services shall be designed using portable language constructs. Ported versions of this software are required to execute on designated GCCS platforms (Sun, HP).

Traceability:
Priority ???

### 3.6.3 Joint Mapping Tool Kit (JMTK) Adaptation Requirements

For Version 3.0, a stand-alone module will be provided to mission application developers to load and index DMA formatted data.

## *3.7 Safety Requirements*

None of the services provided in the Common Support Applications services shall interface with, or defeat the purpose of, safety functions implemented in the host system.

Traceability:
Priority 1

## *3.8 Security and Privacy Requirements*

### 3.8.1 Alert Services Security and Privacy Requirements

Alert Services shall be designed to operate in a “System High” security regimen. The Alert Services software shall rely on the security policy and capabilities of the user system in which it is embedded.

Traceability:
Priority ???

### 3.8.2 Track Correlation Management Services Security and Privacy Requirements

The Track Correlation Management system **shall** maintain classification and releasability information for reports, track attributes, and data source. This system **shall** be capable of operating in all security domains within the constraints of the security certification and accreditation process.

Traceability:
Priority ???

### 3.8.3 Joint Mapping Tool Kit (JMTK) Security and Privacy Requirements

The GCCS/JMTK has no specific security and privacy requirements. GCCS/JMTK will support the marking of appropriate classification, privacy, and copyright levels. System security is assumed to provided by Security Services. DMA will determine data classification and releasability.

### 3.8.4 Message Processing Security and Privacy Requirements

Security policy enforcement is the responsibility of the Trusted Computing Base (TCB). The COE design assumes that COE Layers 1 and 2 will contain COTS products adhering to either the C2 or B1 levels of operational requirements, as defined in the Trusted Computer System Evaluation Criteria. Satisfaction of security requirements needed to adhere to the COE Security Policy are allocated to trusted COE and COTS components. Processes that can be implemented without exemption from security controls will be labeled as untrusted. Untrusted code is not responsible for enforcing security, but must follow the policy enforced by the TCB. The resulting requirements on untrusted code are derived from the COE security policy.

The objective COE will be integrate into systems intended to be evaluated at the B1 or higher evaluation class. Guidelines for developing trusted and untrusted software should be followed to ease the eventual migration to the multilevel secure system required by DoD. Development guidelines for untrusted and trusted software, respectively, are documented in DoD 5200.28-STD series of documents.

### 3.8.4.1 Trusted Software Requirements

Exactly which COE components must be trusted can only be determined based on the COE security architecture. It is the responsibility of the system and application developer to determine how trusted and untrusted COE and COTS components are integrated. The requirements below address functionality that must be trusted in order to meet COE security processing requirements.

MP 3.8.1.1 If the message processor is responsible for appending information labels based upon “actual classification labeling” vice system higher water mark, then it shall demonstrate compliance with the B1 evaluation class in a manner that provides data integrity and security protection as defined in DoD 5200.28-STD.

Traceability:
Priority ???

MP 3.8.1.2 If the Message-Based SRI module evaluates and routes based on classification levels, and is responsible for trusted output then it shall demonstrate compliance with the B1 evaluation class in a manner that provides data integrity and security protection as defined in DoD 5200.28-STD.

Traceability:
Priority ???

MP 3.8.1.3 In a system using target COE and providing C2 security, the Message Set Classification public operation shall provide advisory security labels in support of manual downgrade of messages.

Traceability:
Priority ???

MP 3.8.1.4 In a system using target COE and providing C2 security, the Message Get Classification public operation shall provide advisory security labels in support of manual downgrade of messages.

Traceability:
Priority ???

MP 3.8.1.5 In a system using objective COE and providing B1 security, the Message Set Classification process shall be implemented in a trusted process and shall be valid only when invoked by a trusted subject.

Traceability:
Priority ???

### 3.8.4.2 Untrusted Software Requirements

Untrusted software is impacted by security enforcement imposed by the TCB. The first element of security enforcement is Mandatory Access Control (MAC) on information flow between components: Multilevel security is transparent to untrusted software in that untrusted code has no knowledge of security labels maintained by the TCB. However, MAC in multilevel secure systems restricts data flow between system components. This will impact the way in which various trusted and untrusted COE and COTS components are integrated into the system's architecture. For example, all users of an untrusted application may be required to operate at an application-high security level. The second element of security enforcement is the restriction of privileges for individual components. Untrusted software uses only the standard operating system and supports software services that require no special privileges.

In addition to the security enforcement imposed by the TCB, a secure system provides a small selection of security features that are visible and available to untrusted software. Where appropriate, COE provides interfaces to these features.

The following are general processing requirements for untrusted Message Processing Area:

MP 3.8.2.1 Any distinct untrusted processes in the Message Processing Area (e.g., functions not linked into application code) that communicate with one another shall run at the same security level.

Traceability:
Priority ???

MP 3.8.2.2 Untrusted software shall use only the standard operating system and support software services that require no special privileges.

Traceability:
Priority ???

MP 3.8.2.3 If the underlying COTS software provides security features that are visible to untrusted applications, then untrusted COE components shall make available an interface to those features.

Traceability:
Priority ???

### 3.8.4.3 Accountability

All transactions that occur within the message processor module, and those that occur between the message processor module and external modules will be accounted for. The method for providing this accountability is by use of an audit trail. To support this audit trail, the message processor module shall:

MP 3.8.3.1 Output an audit record for each occurrence of a user definable transaction (user here refers to an authorized administrator with access to system configuration files and audit trail).

Traceability:
Priority ???

MP 3.8.3.2 Record the following with every audit record:

a. Date and time of event

Traceability:
Priority ???

b. Event

Traceability:
Priority ???

c. Security markings

Traceability:
Priority ???

d. Success or failure

Traceability:
Priority ???

e. User ID

Traceability:
Priority ???

f. Duty position/role

Traceability:
Priority ???

MP 3.8.3.3 Record the following with every message-related audit record:

a. Date and time of message origination (DTG)

Traceability:
Priority ???

b. Subject/Message Id

Traceability:
Priority ???

c. Message Originator

Traceability:
Priority ???

d. Message Destination

Traceability:
Priority ???

e. Security Classification (including codewords/nicknames and handling caveats)

Traceability:
Priority ???

f. Message identification and number

Traceability:
Priority ???

MP 3.8.3.4 Provide the capability to audit the following types of events:

a. Beginning and ending of a message database session.

Traceability:
Priority ???

b. Access to messages in the message processing module database.

Traceability:
Priority ???

MP 3.8.3.5 Provide a protection mechanism for audit data such that read and modify access is limited.

Traceability:
Priority ???

### 3.8.4.4 Access

Access rights shall be controlled and supplied by the Security Administration software.

Traceability:
Priority ???

### 3.8.4.5 Labels

Information labels are required to be attached to every object within a system, if that system is required to maintain a relationship between information within the system and the actual classification of the data (see paragraph 3.2.1.3 for additional information). If a system is to be evaluated and accredited to operate at the B1, or higher, level of certification the message processor shall:

MP 3.8.5.1 Attach an information label(s) to each object created.

Traceability:
Priority ???

MP 3.8.5.2 Create information labels IAW DIAM 65-19.

Traceability:
Priority ???

### 3.8.4.6 Marking

Security marking shall be applied to all data when exported to a hardcopy device IAW DIAM 65-19.

Traceability:
Priority ???

### 3.8.4.7 Data Continuity

### 3.8.4.8 Data Integrity

Data integrity shall be retained through protection of data such that the data is not exposed to accidental or malicious alterations or destruction

Traceability:
Priority ???

#### 3.8.4.9 Object Reuse

Object reuse shall be in conformance with DoD 5200.28.

Traceability:
Priority ???

#### 3.8.4.10 Contingency Planning

#### 3.8.4.11 System Architecture

The message processor software module shall conform to the COE architectural design philosophy and constraints.

Traceability:
Priority ???

#### 3.8.4.12 System Integrity

### 3.8.5 Office Automation Security anf Privacy Requirements

The current trend in DII is to build systems in compliance with a common infrastructure made up of interoperable and reconfigurable components. To ensure that components plug-and-play, the infrastructure and target system architectures are standards-based. To reduce life-cycle costs, DII will incorporate commercial off-the-shelf (COTS) components and open systems standards.

From a security standpoint, there are a number of issues given a COTS-based approach. First, the pedigree of COTS products is unknown and thus the assurance and functional capability of the documented (and undocumented) security features and mechanisms are suspect. Without detailed design information, the approach to security risk management, certification, and accreditation of COTS products focuses on testing to see if one can defeat a product’s security mechanisms rather than on design analysis. Common product and standards knowledge and misconfigurations make COTS products more vulnerable to hackers. This threat increases the need to strictly configure and manage systems, since reconfiguration can provide further opportunities for attack. The effectiveness of information security depends on careful configuration of components, continuous security monitoring, and user training.

Security functionality provided by an information system must be complemented by security controls from other disciplines, including physical, administrative, and procedural security. In particular, the operational effectiveness of information security functionality depends on how well it is administered and used, and hence, on operational procedures and user security training. Furthermore, the use of a common infrastructure will result in a greater exposure to attacks and will increase the importance of strictly configuring and managing the infrastructure since reconfiguration could provide new opportunities for attack.

The DII Office Automation software shall be capable of being configured, operated and maintained in accordance with the DII Management Services functional area requirements. These requirements include accountability, availability, confidentiality and integrity. For further definition of these requirements and how they apply to the COTS products selected for the office automation functional area, refer to DII Security Requirements Document.

### 3.8.6 On-Line Support Services Security and Privacy Requirements

OL 3.8.1 On-Line Support services, in determining classification levels, shall take into account the sensitivity of data to be offered and, once implemented, shall comply with Multilevel Security (MLS) standards.

Traceability:
Priority 1

## *3.9 Environment Requirements*

### 3.9.1 Alert Services Environment Requirements

Alert Services must be portable and is required to execute on all hardware-operating system variants of the GCCS platforms.

Traceability:
Priority ???

### 3.9.3 Joint Mapping Took Kit (JMTK) Environment Requirements

Ultimately, the GCCS/JMTK is to be hardware independent and operate on a range of open system platforms running under standards-based operating systems designated by GCCS (Refer to Paragraph 3.10.3.1 below).

### 3.9.4 Message Processing Environment Requirements

### 3.9.4.1 Software requirements

The Message Processor is intended for use across multiple hardware platforms and operating systems in support of the DoD implementation of the Common Operating Environment (COE), a cost reduction strategy affecting development and maintenance of software and Interoperability.

Minimum software requirements for successful hosting are:

- UNIX Operating System
- X11R5
- Motif Windows manager (MIT version)
- Communications front end for receipt and release of record traffic

Discussions with Service representatives have highlighted the need to support message preparation and parsing in the DOS/Windows environment until transition to the GCCS selected product is completed.

## *3.10 Computer Resource Requirements*

### 3.10.2 Track Correlation Management Services Computer Resource Requirements

The TCMS **shall** be compatible with the DII COE hardware platforms.

Traceability:
Priority ???

### 3.10.2.1 Computer Hardware Requirements

Throughput and performance of the Tdb and associated correlation processes **shall** be sufficient to maintain near real time performance with the data arrival rates capable of being presented across the external interfaces listed in Section 3.3.2.2.1. This includes both the automatic correlation throughput, and the distribution across the LAN/WAN.

Traceability:
Priority ???

### 3.10.2.2 Computer Hardware Resource Utilization Requirements

### 3.10.2.3 Computer Software Requirements

### 3.10.2.4 Computer Communications Requirements

The TCMS **shall** support the storage, management, and display of tracks that are shared between WAN activities across the battlespace, local to an organization’s LAN, or restricted to a particular terminal.

Traceability:
Priority ???

### 3.10.2.4.1 Local Terminal

The TCMS **shall** provide backup access to the Tdb server, and shared memory will be restored when necessary due to data loss.

Traceability:
Priority ???

### 3.10.2.4.2 Inter-DB synchronization

The TCMS **shall** support two principle track management servers. In order to prevent loss of data in the event of a server failure, these databases must be synchronized; i.e. hot server backup.

Traceability:
Priority ???

### 3.10.2.4.3 Information Broadcasts

3.10.2.4.3.1 The TCMS **shall** allow the transmission of selected tracks to another location using the Communication Service. All track types, including ambiguities, may be transmitted. The TCMS **shall** permit either one track or a group of tracks to be transmitted.

Traceability:
Priority ???

3.10.2.4.3.2 When transmitting track reports, in support of COP processing, the TCMS **shall** be able to support identifying the tracks by their local track numbers or by their Unique ID.

Traceability:
Priority ???

3.10.2.4.3.3 The TCMS **shall** provide the option of sending the track data in compressed or expanded format. Compressed format reports **shall** contain additional information relevant to the individual track, while expanded format **shall** contain additional information.

Traceability:
Priority ???

3.10.2.4.3.4 The TCMS **shall** provide the option to send history information with the track report or to send only the last reported position for the track. The TCMS **shall** support sending only basic track information or an expanded set of information.

Traceability:
Priority ???

#### 3.10.2.4.4 Information Alerts

3.10.2.4.4.1 Alert management: The TCMS **shall** provide a centralized rule base to support track alert management. The concept is to remove the burden of identifying alerts from the clients and manage this task from the central server. Each application **shall** be capable of adding/inputting alert rules, the server **shall** identify them and alert the application of exceptions when they occur. Alerts may be overridden or augmented by mission applications.

Traceability:
Priority ???

3.10.2.4.4.2 Special Interest: The TCMS **shall** provide a database that supports the generation of reports for tracks that are marked as being of special interest. The TCMS **shall** maintain a status of “suspect” and “nonsuspect” for operator-selected tracks. The designation of “suspect” will indicate that these tracks are of special interest. This designation may be applied and removed by appropriate authorities in the network. An ALERT field in a track’s edit window will be used to make this designation.

Traceability:
Priority ???

3.10.2.4.4.3 The TCMS **shall** also provide a mechanism for transmitting the suspect/nonsuspect indication between activities via the Communication Service.

Traceability:
Priority ???

3.10.2.4.4.4 The TCMS **shall** provide for identification of suspect tracks on the tactical display.

Traceability:
Priority ???

## 3.10.3 Joint Mapping Tool Kit (JMTK) Computer Resources Requirements

The GCCS/JMTK will be compatible with GCCS-specified platforms and operating systems.

Traceability:
Priority ???

### 3.10.3.1 Computer Hardware Requirements

There is no hardware specific to the GCCS/JMTK. The GCCS/JMTK will be an opern system capable of running on any GCCS COE approved platform. The approved Commercial Off-the-Shelf (COTS) platforms for GCCS 2.0 are Hewlett Packard (HP) 9000/7000 series workstations and SUN SPARC 10/20/1000/2000 series workstations running under UNIX based operating systems. Future GCCS machines in tentative order are: RISC 6000, DEC Alpha, and Silicon Graphics Incorporated (SGI).

### 3.10.3.2 Computer Hardware Resource Utilization Requirements

The developers of the GCCS/JMTK components have provided their minimum requirements for running their software. The workstations need 64 megabytes of RAM and two gigabytes of hard disk storage.

### 3.10.3.3 Computer Software Requirements

The currently approved operating systems are Solaris 2.4, HP/UX 9.07, and Windows/NT 3.51. Future operating system upgrades anticipated include Solaris 2.5, AIX 4.1, Digital Unix, and SGI IRIX. In addition to the operating system software, the following software items are recommended for using the GCCS/JMTK:

- X-Windows X 11R5

- Motif: Version 1.2 or most recent
- C compilers current versions for HP, Sun, and the GNU compiler

### 3.10.3.4 Computer Communications Requirements

The GCCS hardware and software components will be configured to meet specific user needs. MCG&I data can be accessed through GCCS/JMTK functional server via local access, LAN/WAN access or Global Broadcast techniques. WAN access allows for access via the Global Broadcast System and DMA's Global Geospatial Information and Services program. The data services domains have two major components which are Accesses/Gateways and Management. GCCS/JMTK computer communications requirements are being considered in the design of the GCCS architecture.

## 3.10.4 Message Processing Computer Resource Requirements

### 3.10.4.1 Computer Hardware Requirements

COE software capabilities will be developed for the following platforms (A platform is a selected pairing of Computing Hardware and an Operating System):

a. Army CHS product list
b. Navy TAC IV product list

### 3.10.4.2 Computer Hardware Resource Utilization Requirements

Minimum hardware requirements for successful hosting of the current implementation are:

- 32 MB Random Access Memory (RAM)
- 30 MB hard disk space available

### 3.10.4.4 Computer Communications Requirements

MP 3.13.1 The message processing module shall use UNIX and DCE computer communications services to route messages, journal messages, and parsed data to the appropriate directory or application.

Traceability:
Priority ???

MP 3.13.2 The message processing module shall use the COE Communications Services Area to route messages across a Wide Area Networks (e.g., Mobile Subscriber Equipment (MSE) and Combat Net Radio (CNR)).

Traceability:
Priority ???

## 3.10.6 On-Line Support Services Computer Resource Requirements

### 3.10.6.1 Computer Hardware Requirements

OL 3.10.1.1 The On-Line Support segment shall run on all platforms approved for GCCS COE implementation.

Traceability:
Priority 1

### 3.10.6.4 Computer Communication Requirements

OL 3.10.4.1 The On-Line Support segment shall run on isolated terminals as well as on LANs and WANs.
Traceability:
Priority 1

## *3.11 Software Quality Factors*

### 3.11.1 Alert Services Quality Factors

Alert Services must be designed using portable language constructs. Ported versions of this software are required to execute on all hardware-operating system variants of the GCCS platforms.
Traceability:
Priority ???

### 3.11.3 Joint Mapping Tool Kit (JMTK) Software Quality Factors

The software quality factors that have already been put in place by the Military Services for CHART, CMTK and TEM that are represented in the GCCS/JMTK will be assumed.

### 3.11.5 Office Automation Software Quality Factors

Office Automation capabilities shall be portable and reusable.
Traceability:
Priority 1

## *3.12 Design and Implementation Constraints*

### 3.12.1 Alert Services Design and Implementation Constraints

As Alert Services is to be implemented as common software module within the DII COE, the developers can make no assumptions about the “look and feel” of the user interface for the system in which it eventually will be embedded. Therefore, the “Display” portion of Alert Services must be implemented as a generic display tool, to be used solely for demonstration purposes, testing, and as a coding example for Alert Services clients.
Traceability:
Priority ???

### 3.12.2 Track Correlation Management Services Design and Implementation Constraints

The TCMS **shall** consist of a client-server architecture. Two versions of the primary server **shall** be supported on the same LAN with database commonality. This is necessary to support master-to-master data exchange. Two separate systems **shall** be capable of existing in two separate states and **shall** therefore utilize independent servers to support event by event communications on each.
Traceability:
Priority ???

### 3.12.2.1 Structure independent data access

The APIs **shall** be designed in a manner that supports longevity and compatibility. This **shall** be achieved through a design which creates and enforces a barrier between data structures and the calling application. The calling routine **shall** require no knowledge of the systems data structures.

Traceability:
Priority ???

## 3.12.3 Joint Mapping Tool Kit (JMTK) Design and Implementation Constraints

GCCS/JMTK will be compatible with GCCS-specified platforms and operating systems. Presently, GCCS COE release 2.X consists of Sun Solaris Version 2.4 and HP UX Version 9.0.7 with OS compatible versions of X-windows and Motif. The goal is that GCCS/JMTK be compatible with GCCS COE documentation and guidelines and eventually support the GCCS objective architecture.

## 3.12.4 Message Processing Design and Implementation Constraints

MP 3.12.1 The message processing module shall provide upwardly compatible interfaces between COE versions of the Message Processing Area and application programs.

Traceability:
Priority ???

MP 3.12.2 The message processing module shall provide upwardly compatible functional services Message Processing Area in COE versions to applications programs.

Traceability:
Priority ???

MP 3.12.3 The message processing module shall be portable across Government Furnished Equipment/ Government Furnished Information (GFE/GFT) common hardware and software platforms.

Traceability:
Priority ???

MP 3.12.4 The design and implementation of the message processing module shall conform to the COE architecture.

Traceability:
Priority ???

MP 3.12.5 The message processing module shall incorporate an open systems architecture design, in accordance with that defined by the Global Command and Control Systems (GCCS) Common Operating Environment (COE) to allow integration with other applications/systems.

Traceability:
Priority ???

MP 3.12.6 The message processing module shall operate in a Distributed Computing Environment (DCE).

Traceability:
Priority ???

MP 3.12.7 The message processing module shall allow for future growth/expansion and portability through early definition and stability of Application Programmer Interfaces (API).

Traceability:
Priority ???

MP 3.12.8 The message processing module shall be designed to support operations of selected modules (those required for message generation) in a DOS/Windows environment.

Traceability:
Priority ???

### 3.12.5 Office Automation Design and Implementation Constraints

Versions of the Office Automation functional area modules shall operate on the required DII hardware platforms running the specified operating systems. Currently, DII supports the following platforms and operating systems:

1. Hewlett-Packard (HP) 900/700 Series workstations running HP-UX v9.01 and HP-UX v10.0
2. Sun Microsystems (Sun) SPARC workstations running Solaris v2.4 and v2.5
3. Intel workstations running Windows NT and Windows 95 (supported as clients only).

Therefore, office automation products which are selected for use in the DII COE must be available for these platforms.

Traceability:
Priority 1

### 3.12.6 On-Line Support Services Design and Implementation Constraints

OL 3.12.1 The On-Line Support services shall be implemented by approved system APIs only.

Traceability:
Priority 1

OL 3.12.2 The On-Line Support services shall be upgradable to incorporate future help additions to attain the goal of software reusability.

Traceability:
Priority 1

OL 3.12.3 For future versions, the On-Line Support services shall be backward-compatible.

Traceability:
Priority 2

## *3.13 Personnel-Related Requirements*

### 3.13.3 Joint Mapping Tool Kit (JMTK) Personnel-Related Requirements

The GCCS/JMTK will conform to accepted human factors guidelines and practices to support ease of use, training, and performance.

### 3.13.4 Message Processing Personnel-Related Requirements

MP 3.14.1 All message preparation instructions and help text shall be provided to the drafter/user by the message processing module.

Traceability:
Priority ???

MP 3.14.2 The message processing module shall provide on-line and interactive help (context sensitive).

Traceability:
Priority ???

MP 3.14.3 Service unique help shall be provided if adequate information is supplied by the services in a format compatible with USMTF CDBS standard.

Traceability:
Priority ???

MP 3.14.4 The human interface shall be developed IAW the DoD Human Interface Design Handbook.

Traceability:
Priority ???

## *3.14 Training-Related Requirements*

### 3.14.3 Joint Mapping Tool Kit (JMTK) Services Training-Related Requirements

Training for all GCCS/JMTK user personnel must be in accordance with the GCCS Training Plan through approved GCCS training courses.

### 3.14.6 On-Line Support Services Training-Related Requirements

Refer to Requirements OL 3.2.3.1 through OL 3.2.3.3.

## *3.15 Logistics-Related Requirements*

### 3.15.3 Joint Mapping Tool Kit (JMTK) Logistics-Related Requirements

DMA will provide software support for the GCCS/JMTK. The DISA Engineering Office will distribute the GCCS/JMTK.

### 3.15.5 Office Automation Logistics-Related Requirements

All software shall be made available and distributed in accordance with the DII COE Integration and Runtime Environment Specification, V2.0.

Traceability:
Priority 1

## *3.16 Other Requirements*

### 3.16.5 Office Automation Other Requirements (Interoperability Requirements)

Interoperability is the ability to move data and information across networks. One of the reasons for migrating to a reduced number of systems is to improve interoperability between systems. With many different systems performing similar functions, it is an extremely difficult task to ensure that all the system deployed will be able to inter operate. By reducing the variety of systems proliferated, the problem of interoperability between systems is also reduced to a more manageable challenge.

In addition to integrating the office automation capabilities it is also important that the data produced by the office automation modules can be imported and exported in a suitable format. The requirements for the import and export of data within the individual office automation packages are contained within the functional requirements for each package.

The DII Office Automation software suite shall inter-operate such that each of the packages can exchange data and information across the network. In addition, the DII Office Automation software shall inter-operate, as needed, with all other DII functional areas.

Traceability:
Priority 1

## *3.17 Packaging Requirements*

### 3.17.1 Alert Services Packaging Requirements

#### 3.17.1.1 Alert Services Shipping Protection Provisions

The developer shall prepare all items for shipment with preservation packaging and marking such that protection is provided against deterioration and physical damage during shipment and handling from the source of supply to the ultimate destination.

Traceability:
Priority ???

#### 3.17.1.2 Alert Services Media

All releases from the developer shall be provided on removable storage media (e.g., tape, CD-ROM, or magneto-optical disks) consistent with GCCS equipment. The developer shall provide all releases in both source and object format, as well as segmented in accordance with the GCCS Integration Standard.

Traceability:
Priority ???

All software shall be delivered in accordance with the DII COE Integration **-** Runtime Environment Specification, V2.0 (Draft).

Traceability:
Priority 1

## *3.18 Precedence and Criticality of Requirements*

The order of precedence or criticality indicating the relative importance of the requirements in this specification are identified and prioritized in Section 5, Requirements Traceability.